Assessment of Agency Compliance with Enterprise Security Standards

Summary Report

George Bakolia, State Chief Information Officer

Ann Garrett, Chief Information Security Officer

Agenda

- Project Background
- Approach and Methodology
- Summary of Findings
  - Charts
  - Major Findings
  - High Level Recommendations
  - Cost Estimates
- Questions

Project Background

Project Overview

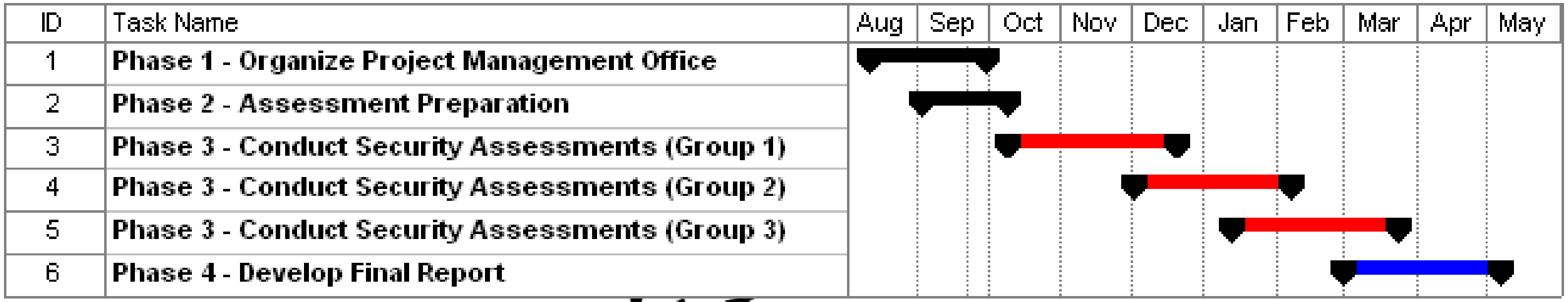
- In response to North Carolina Session Law 2003-153, the State of North Carolina conducted a statewide security assessment of all Executive Branch agencies
- Assessment process was intended to provide key-decision makers with:
  - Global view of the security status of agencies
  - Detailed findings sufficient to permit State to prioritize and budget for required remediation efforts
- Assessment was based on the North Carolina Security Framework which is based on ISO17799 standards

Project Overview (Cont.)

- Assessment requirements for each agency included:
  - Rate of compliance with the standards
  - Security organization
  - Network security architecture
  - Current information technology security expenditures
  - Remediation costs
- The IRMC and State CIO must submit a public report to the Joint Legislative Commission on Governmental Operations by May 4, 2004, including:
  - Summary of the assessment results
  - Estimates of additional funding needed to bring agencies into compliance
- The IRMC and State CIO must provide updated assessment information by January 15 of each subsequent year

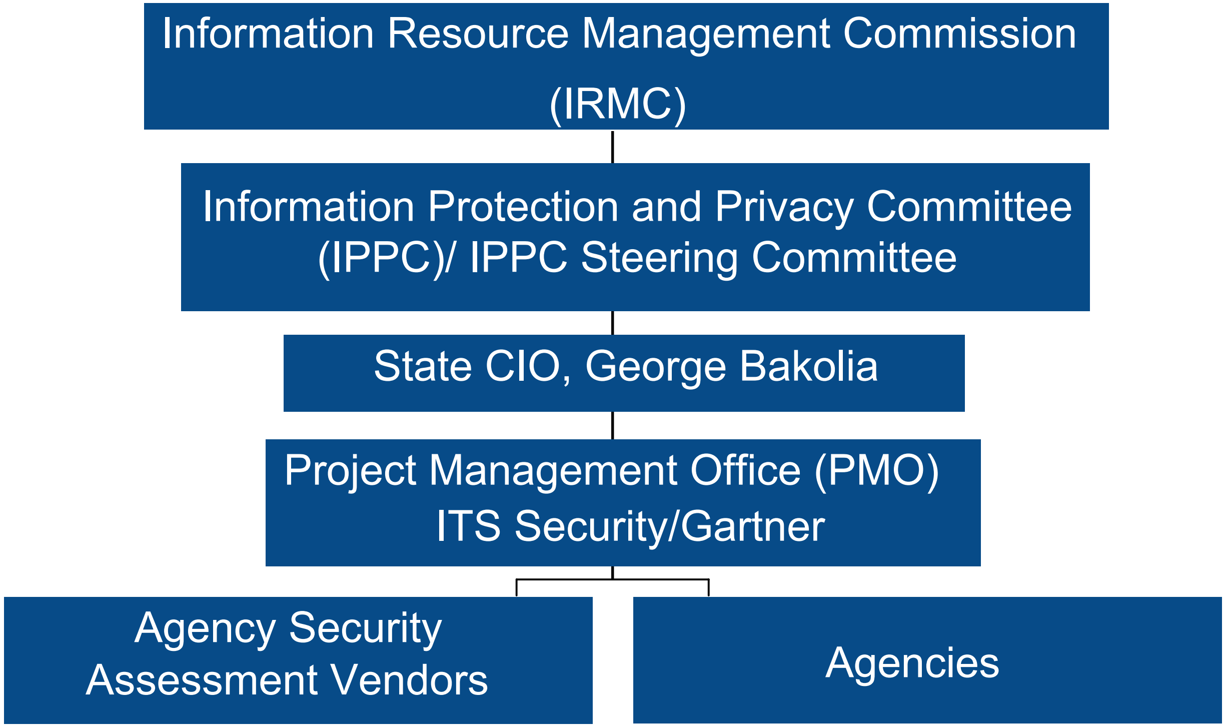
Project Timeline

- 4-Phase Project:
  - Phase 1: Organize Project Management Office (PMO)
  - Phase 2: Assessment Preparation
  - Phase 3: Conducted Security Assessments:
    - Group 1 - October 13 – December 4
    - Group 2 - December 2 – February 3
    - Group 3A - January 12 – March 24
    - Group 3B - January 28 – March 24
  - Phase 4 - PMO identify statewide security risks, develop cost and resource estimates for statewide corrective action.
- Completed project on time and under budget



ID	Task Name
1	**Phase 1 - Organize Project Management Office**
2	**Phase 2 - Assessment Preparation**
3	**Phase 3 - Conduct Security Assessments (Group 1)**
4	**Phase 3 - Conduct Security Assessments (Group 2)**
5	**Phase 3 - Conduct Security Assessments (Group 3)**
6	**Phase 4 - Develop Final Report**

Security Project Reporting Structure



Information Resource Management Commission (IRMC)

Information Protection and Privacy Committee (IPPC)/ IPPC Steering Committee

State CIO, George Bakolia

Project Management Office (PMO)
ITS Security/Gartner

Agency Security Assessment Vendors

Agencies

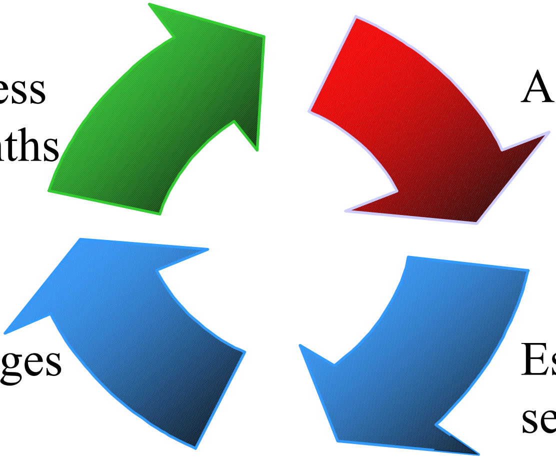
Project Responsibilities

Participants	Primary Responsibilities
Project Management Office – ITS / Gartner	• Develop all project tools and templates • Manage assessment project • Develop preliminary and extrapolated cost estimates • Develop final recommendations and final cost estimates • Train vendors in use of tools and templates • Project reporting
Vendors	• Conduct assessments of assigned agencies • Project Management/Reporting to PMO (status, issues, etc.)
Agencies	• Led by agency security liaison • Prepare for assessments • Provide documentation • Participate in assessments

Approach and Methodology

Assessment Process Definition

- An ongoing process of defining, selecting, designing, collecting, analyzing, and interpreting the information to measure performance against standards



Assess agencies

Estimate budget to mitigate security-related risks

Implement changes

Re-assessment process begins in 18-24 months

Project Approach

- There are four ways to capture security information. The State's Security Assessment Project used the first two:

Policy standard and guidelines review – Assessment team conducts a paper review

"Eyes-on" security review– Reconciliation of security policies v. deployment; typically involves spot checking of key systems to verify compliance

"Hands-on" security review – Detailed audit of asset configuration

Vulnerability assessment– Series of sanctioned attacks designed to probe system

Assessment Focus Areas

- The assessment methodology leverages the ISO 17799 framework

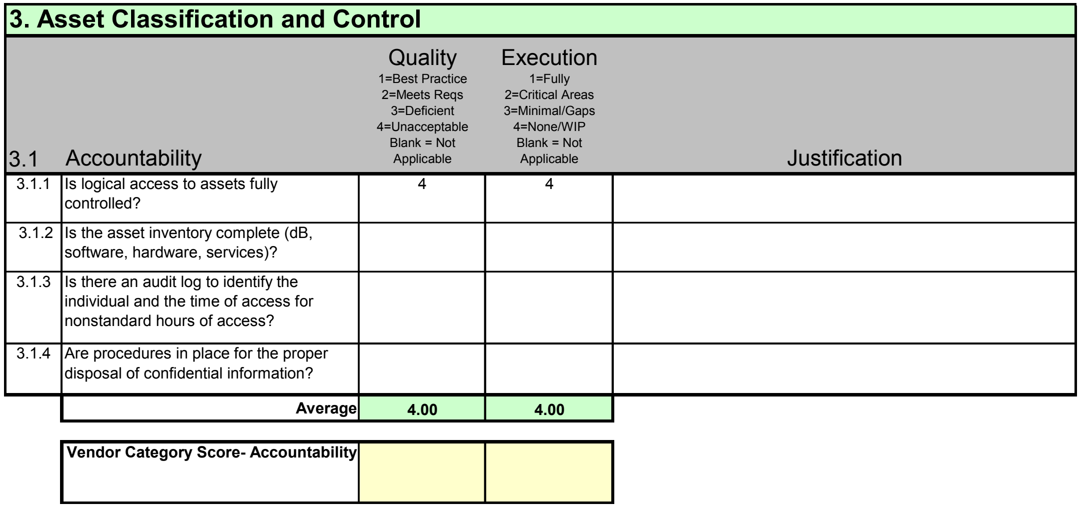
Security Policy	Management support, commitment, direction in accomplishing information security goals
Organizational Security	Need for management framework that creates, sustains, and manages security infrastructure of organization
Asset Classification and Control	Ability of security infrastructure to protect organizational assets
Personnel Security	Organization’s ability to mitigate risk inherent in human interactions
Physical Security	Risk inherent to organizational premises
Communications & Operations	Organization’s ability to ensure correct and secure operation of its assets

Assessment Focus Areas (Cont.)

Access Administration	Organization’s ability to administratively control access to assets based on business and security requirements
Access Technology	Organization’s ability to control access to technology-specific assets based on business and security requirements
Applications Development & Maintenance	Organization’s ability to ensure appropriate information system security controls are incorporated and maintained
Business Impact / Continuity	Organization’s ability to counteract interruptions to normal operations
Compliance	Organization’s ability to remain in compliance with regulatory, statutory, contractual and security requirements.

Security Assessment Tool

- The assessment vendors worked with the agencies to complete the tool
- Scoring was based on a scale of 1 to 4
- Scoring has two key components: Quality and Execution
- Each category consisted of sub-sections with related questions
- Question scores were averaged, providing an overall category score
- Category scores were averaged providing an overall Agency score



3. Asset Classification and Control

3.1	Accountability	Quality 1=Best Practice 2=Meets Reqs 3=Deficient 4=Unacceptable Blank = Not Applicable	Execution 1=Fully 2=Critical Areas 3=Minimal/Gaps 4=None/WIP Blank = Not Applicable	Justification
3.1.1	Is logical access to assets fully controlled?	4	4	
3.1.2	Is the asset inventory complete (dB, software, hardware, services)?			
3.1.3	Is there an audit log to identify the individual and the time of access for nonstandard hours of access?			
3.1.4	Are procedures in place for the proper disposal of confidential information?			
	Average	**4.00**	**4.00**	
	Vendor Category Score- Accountability			

Quality	Execution
1=Best Practice	1=Fully
2=Meets Reqs	2=Critical Areas
3=Deficient	3=Minimal/Gaps
4=Does Not Meet Reqs	4=None/WIP
Blank = Not Applicable	Blank = Not Applicable

Assessment Groupings

Assessment Group 1	
Agency	Vendor
Department of Administration	HCS Systems, Inc.
Department of Corrections	CIBER, Inc.
Department of Environment & Natural Resources	Secure Enterprise Computing
Department of Health & Human Services	Ernst and Young, LLP
Department of Labor	Alphanumeric Systems, Inc.
Dept of Transportation	Unisys Corporation
Office of Information Technology Services (ITS)	Pomeroy IT Solutions
Office of the Secretary of State	Alphanumeric Systems, Inc.
Office of the State Auditor	Cii Associates, Inc.
Wildlife Resources Commission	Secure Enterprise Computing

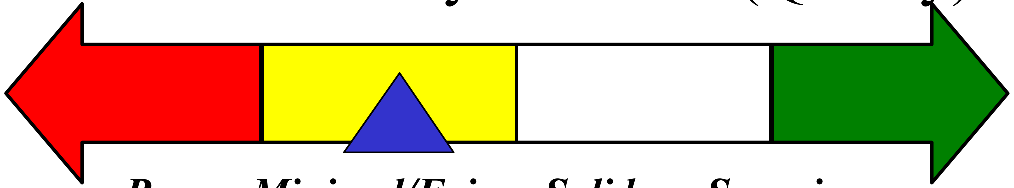
Assessment Group 2	
Agency	Vendor
Community College System	Secure Enterprise Computing
Department of Agriculture	Cii Associates, Inc.
Department of Commerce	Alphanumeric Systems, Inc.
Department of Crime Control	CIBER, Inc.
Department of Insurance	Cii Associates, Inc.
Department of Juvenile Justice & Delinquency Pre	HCS Systems, Inc.
Department of Public Instruction	Pomeroy IT Solutions

Assessment Group 3	
Agency	Vendor
Department of Cultural Resources	Cii Associates, Inc.
Department of Justice	Pomeroy IT Solutions
Department of Revenue	HCS Systems, Inc.
Department of State Treasurer	Cii Associates, Inc.
Employment Security Commission	Secure Enterprise Computing
Office of State Budget and Management	CIBER, Inc.
Office of State Controller	Unisys Corporation
Office of State Personnel	CIBER, Inc.
Office of the Governor	Alphanumeric Systems, Inc.
Office of the Lieutenant Governor	Alphanumeric Systems, Inc.

Summary of Findings

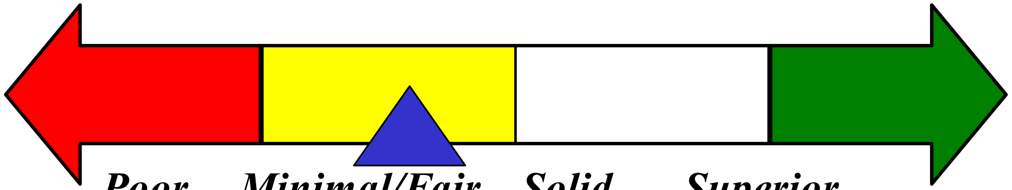
Assessment Scoring Distribution

Planned Security Practices (Quality)



Poor *16%* | *Minimal/Fair* *60%* | *Solid* *20%* | *Superior* *4%*

Actual Security Practices (Execution)

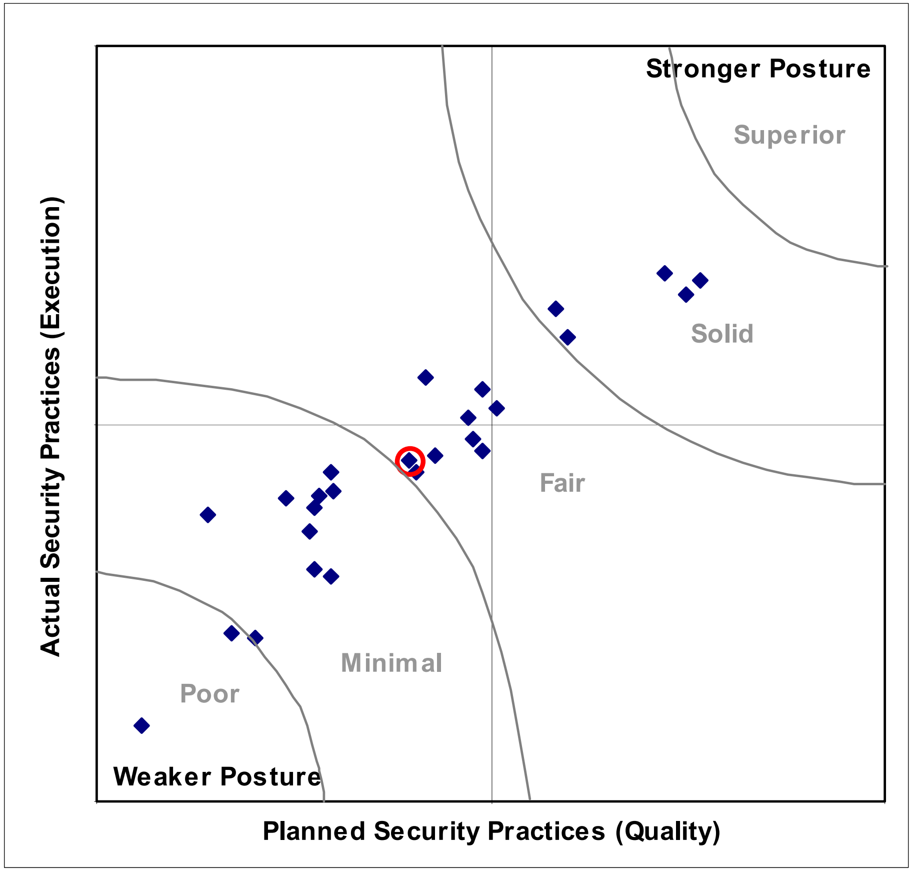


Poor *12%* | *Minimal/Fair* *52%* | *Solid* *36%* | *Superior* *0%*

Agency Security Posture

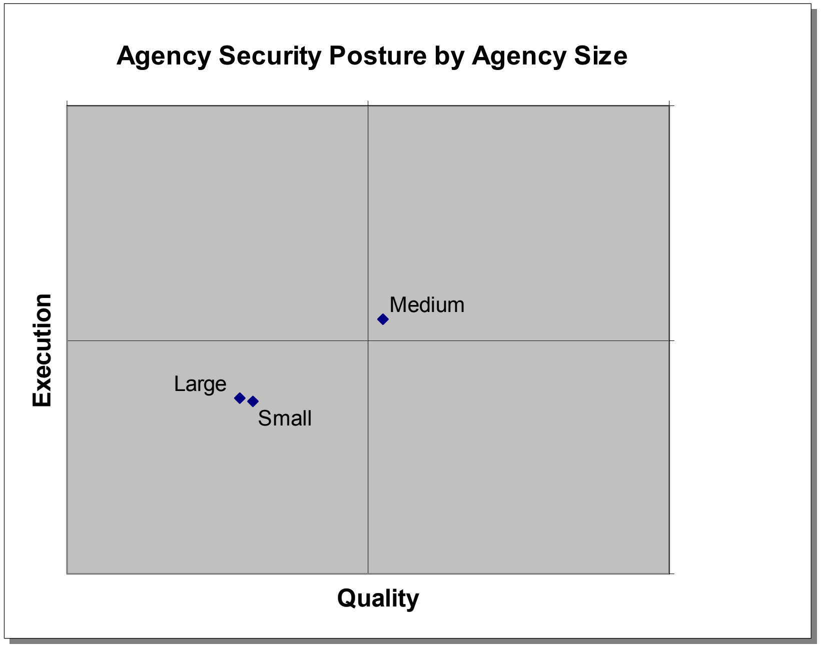
Assessment Score	Posture
1.00 to 1.19	**Superior**
1.20 to 1.39	**Superior**
1.40 to 1.59	**Superior**
1.60 to 1.78	**Solid**
1.80 to 1.99	**Solid**
2.00 to 2.19	**Solid**
2.20 to 2.39	**Solid**
2.40 to 2.59	**Minimal/Fair**
2.60 to 2.79	**Minimal/Fair**
2.80 to 2.99	**Minimal/Fair**
3.00 to 3.19	**Minimal/Fair**
3.20 to 3.39	**Poor**
3.40 to 4.00	**Poor**

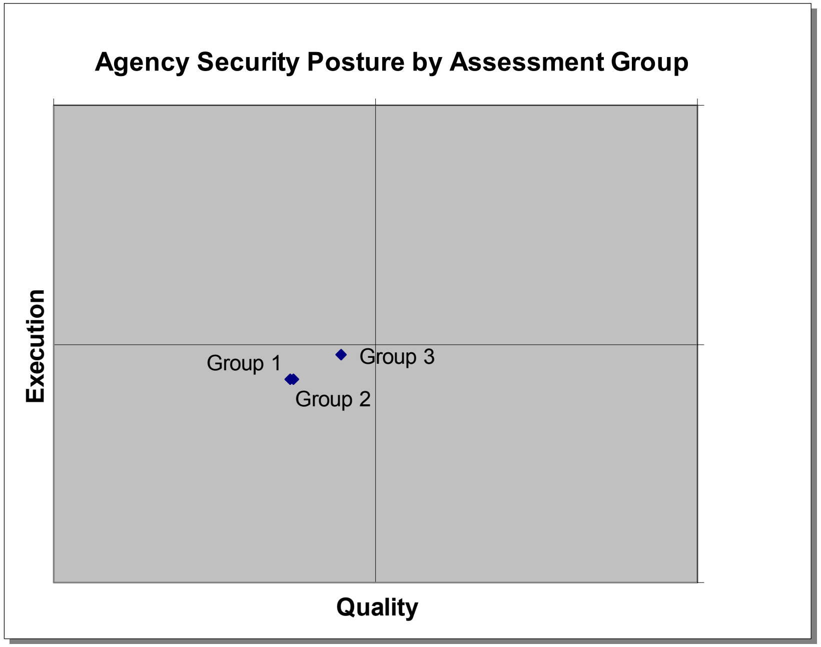
Assessment Scoring Summary



Note: The circle indicates the State average for the agencies assessed in the study

Average Security Scores

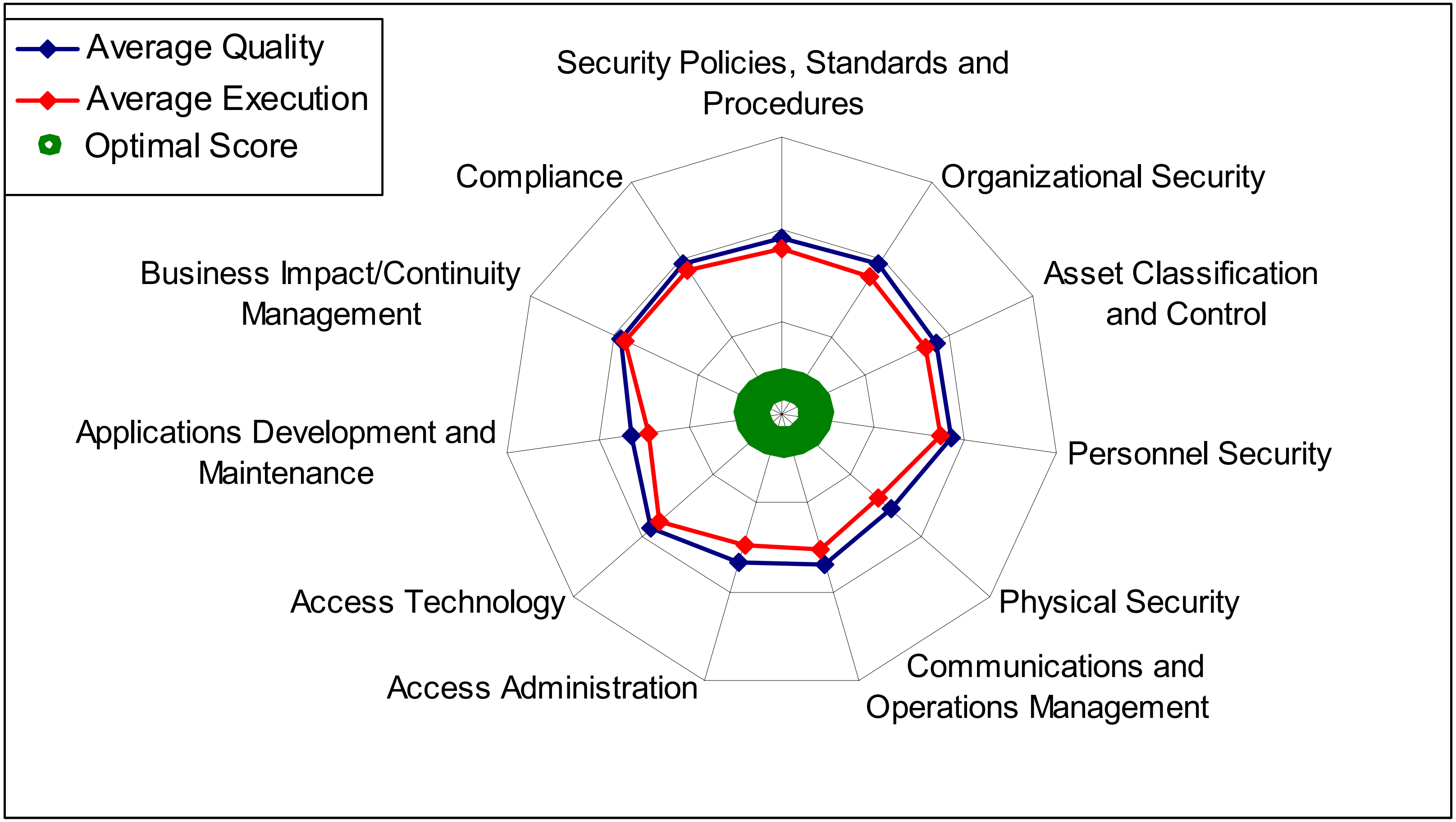




Agency Size	Average Quality	Rating	Average Execution	Rating
Large	3.15	Minimal/Fair	2.88	Minimal/Fair
Medium	2.43	Solid	2.35	Solid
Small	3.10	Minimal/Fair	2.89	Minimal/Fair

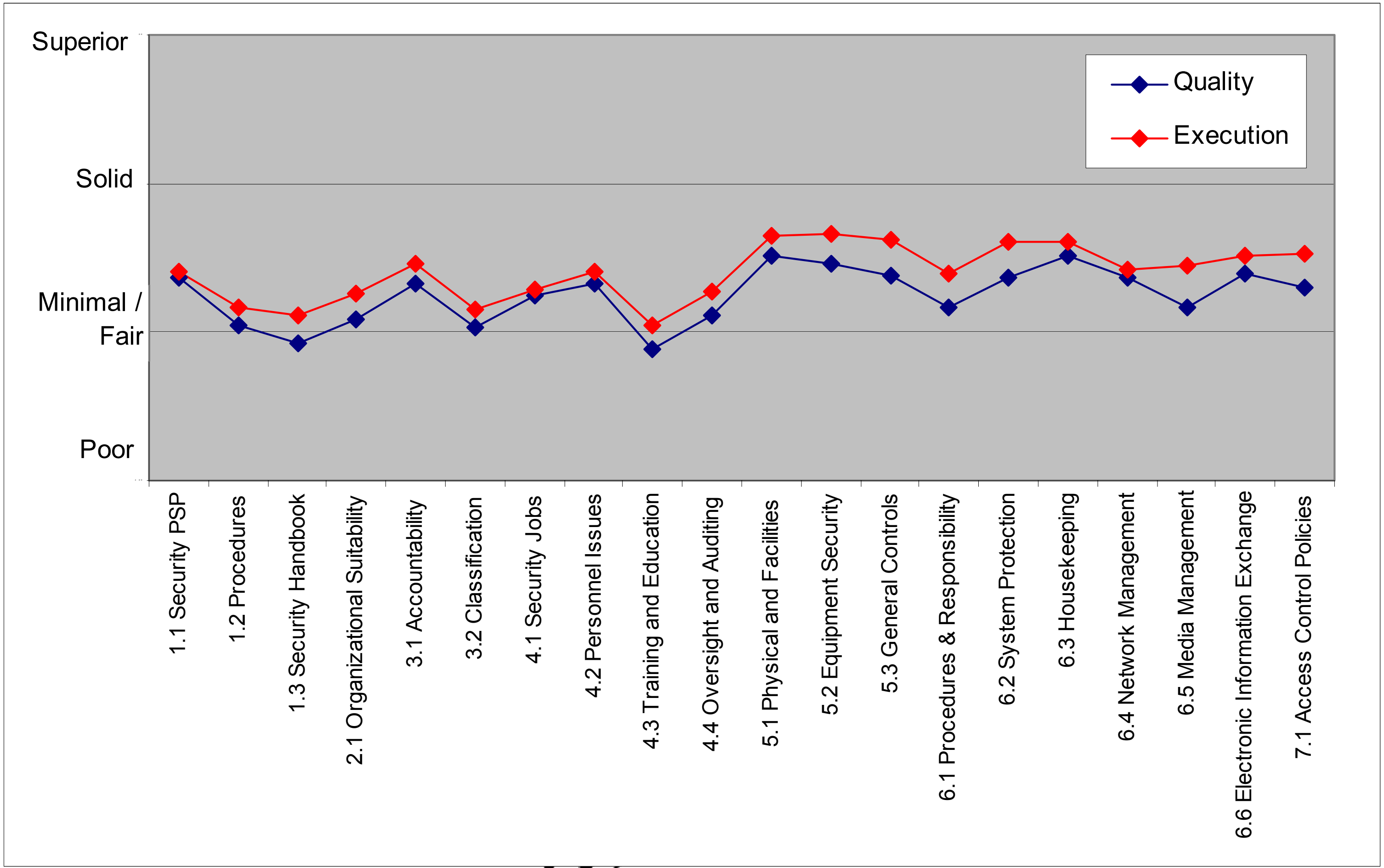
Group	Average Quality	Rating	Average Execution	Rating
1	2.88	Minimal/Fair	2.72	Minimal/Fair
2	2.89	Minimal/Fair	2.71	Minimal/Fair
3	2.65	Minimal/Fair	2.52	Minimal/Fair

Statewide Average Security Scores by Category



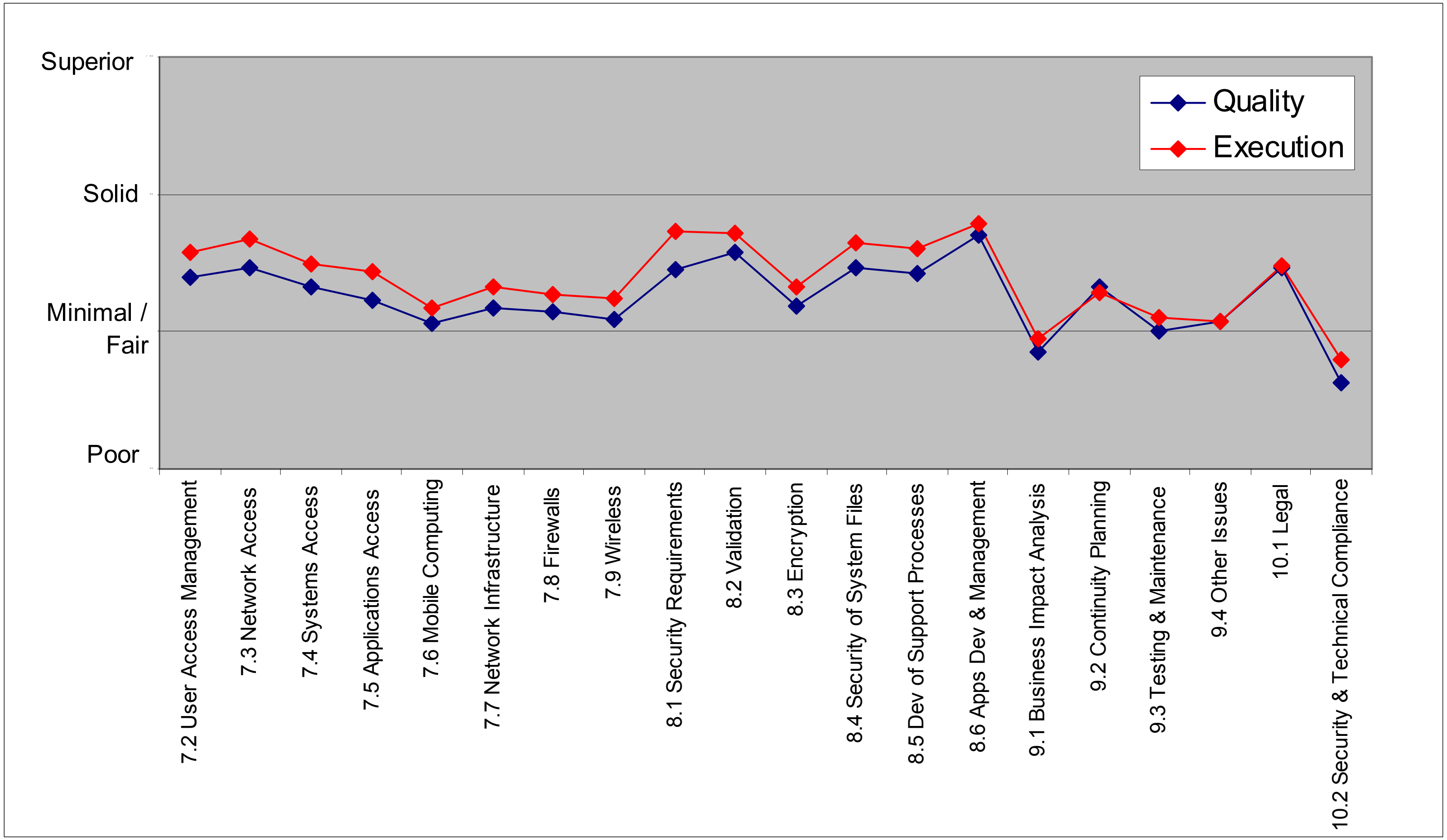
Statewide Average Security Scores by Subcategory

Quality and Execution scores for the 40 sub-categories encompassed in the assessment framework



NC @ your service
www.ncgov.com

Statewide Average Security Scores by Subcategory (Cont.)



Notable Practices

- Security Importance (~100%)
- Removal of Unauthorized Modems (88%)
- Removal of Undesirable Accounts (85%)
- Virus Prevention (84%)
- Keys and Access Cards (81%)
- Security Framework (62%)

Opportunities for Improvement

- Insufficient Funding (~100%)
- Insufficient Staffing (84%)
- Lack of Security Training & Experience (76%)
- Outdated Desktop Operating Systems (72%)
- Outdated and Missing Business Continuity Plans (69%)
- Gaps in Agency Border / Perimeter Defense (64%)
- Deficient Policies, Standards, and Procedures (60%)

Summary Recommendations

Enterprise Recommendations

E1: Increase Funding to enhance the Enterprise Security Program

E2: Complete Statewide Security Policies, Standards, and Procedures

E3: Improve Security Awareness and Training

E4: Improve Risk Management and Update Business Continuity Plans

Agency Recommendations

A1: Increase funding to agencies

A2: Improve Agency Security Policies, Standards, and Procedures

A3: Increase Level of Security Staffing

A4: Improve Security Awareness and Training

A5: Replace Outdated Desktop Operating Systems

A6: Improve Agency Border/Perimeter Defense

A7: Improve Risk Management and Update Business Continuity Plans

Statewide Security Spending

"The average organization spent 7% of revenue on IT in 2003. Gartner estimates that the average organization spent 5.4% of its IT budget on security in that same period. Thus, security spending will consume an average of 0.38% of revenue, annually. Disaster recovery spending was an incremental 3-4% during the same period (or .2% of revenue)"

Source: Gartner, Inc.

	Actual		Recommended		Difference
Statewide Security Spending	$14,015,968	0.15%	$34,595,000	0.38%	$20,579,000
Statewide BCP Spending	$5,128,061	0.06%	$18,208,000	0.20%	$13,080,000

Total Agency Operating Budget $9,103,912,379

Summary Costs by Finding

		Enterprise		Agency		Total	
Finding	**Recommendation**	**Total Initial Outlay**	**Ongoing Operating Costs**	**Total Initial Outlay**	**Ongoing Operating Costs**	**Total Initial Outlay**	**Total Ongoing Operating Costs**
Insufficient Funding	E1: Increase Funding to Enhance Enterprise Program Office	2,026,400	1,821,360			2,026,400	1,821,360
	A1: Increase Funding to Agencies				15,196,640		15,196,640
	Subtotal					2,026,400	17,018,000
Deficient and Absent Policies, Standards, and Procedures	E2: Complete Statewide Security Framework	387,200	35,000			387,200	35,000
	A2: Improve Agency Security Policies, Standards, and Procedures			1,542,800	364,000	1,542,800	364,000
	Subtotal					1,930,000	399,000
Insufficient Levels of Staffing	A3: Increase Level of Security Staffing			2,144,800	2,144,800	2,144,800	2,144,800
Security Experience is Lacking	E3: Improve Enterprise Security Awareness and Training	504,000	205,600			504,000	205,600
	A4: Improve Agency Security Awareness and Training			431,200	436,800	431,200	436,800
	Subtotal					935,200	642,400
Outdated Desktop Operating Systems	A5: Replace Outdated Desktop Operating Systems			38,820,000		38,820,000	
Gaps in Agency Border / Perimeter Defense	A6: Improve Agency Border / Perimeter Defense			1,544,880	374,800	1,544,880	374,800
Outdated and Incomplete Risk and Business Continuity Management	E4: Improve Risk Management and Business Continuity Plans	2,032,800	1,307,990			2,032,800	1,307,990
	A7: Improve Risk Management and Business Continuity Plans			3,466,800	11,771,910	3,466,800	11,771,910
	Subtotal					5,499,600	13,079,900
	Totals:	**4,950,400**	**3,369,950**	**47,950,480**	**30,288,950**	**52,900,880**	**33,658,900**

Bottom Line

- Year after year, the State has under-funded security, resulting in cumulatively increasing its risk of loss of confidentiality, integrity or availability of State assets
- Many agencies are doing what they can to protect themselves within their constrained budgets
- The State needs to dramatically increase funding for security, to achieve a steady-state of security
- Centralization of the planning, standardization, and administration will enable economies of scale and will ensure more efficient responses to threats
- The Agencies need to build on the centralized standards for their specific needs

Questions?